

# [UNIX] Cross Site Scripting in PsychoStats

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0105.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 12/27/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 27 Dec 2004 16:41:00 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Cross Site Scripting in PsychoStats

---

## SUMMARY

<<http://www.psychostats.com/>> PsychoStats is "a statistics generator for games. Currently there is support for a handful of Half-Life "MODs" including Counter-Strike, Day of Defeat, and Natural Selection. PsychoStats gathers statistics from the log files that game servers create by reading through the logs and then calculating detailed statistics for players, maps, weapons and clans. These detailed statistics are stored in a MySQL database which are then viewed online from your website using a set of PHP web pages". A cross site scripting vulnerability exists in Jason Morriss's PsychoStats 'login' parameter.

## DETAILS

Vulnerable Systems:

\* PsychoStats version 2.2.4

Immune Systems:

\* PsychoStats version 2.2.4b

Cross Site Scripting:

The vulnerability exists due to user supplied input not being checked properly. Below is an example.

Securiteam: [UNIX] Cross Site Scripting in PsychoStats

[http://www.example.com/stats/login.php?login=\[XSS\]](http://www.example.com/stats/login.php?login=[XSS])

This vulnerability could be used to steal cookie based authentication credentials within the scope of the current domain, or render hostile code in a victim's browser.

Solution:

The vendor was contacted, responded very promptly and said he will be addressing the issue soon and has released an updated version of the software: <<http://www.psychostats.com/forums/viewtopic.php?t=11022>>  
<http://www.psychostats.com/forums/viewtopic.php?t=11022>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@gulftech.org>>  
GulfTech Security.

The original article can be found at:

<[http://www.gulftech.org/?node=research&article\\_id=00057-12222004](http://www.gulftech.org/?node=research&article_id=00057-12222004)>  
[http://www.gulftech.org/?node=research&article\\_id=00057-12222004](http://www.gulftech.org/?node=research&article_id=00057-12222004)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.